اینترنت مخفی ایران:

آدرس دهی خاص در شبکه ملی

Collin Anderson (@cda)[1]

در حالی که سازمان های گوناگون بودجه های هنگفتی برای تولید کنندگان و ارائه دهندگان سرویس جهت جریان آزاد اطلاعات هزینه می کنند، اطلاعات کمی در رابطه با زیرساخت شبکه و امکانات جمهوری اسلامی در زمینه شبکه و اینترنت موجود است. در انظار عمومی و اطلاعات در دسترس نیز شایعات بیش از واقعیات خودنمایی می کنند. در طول تحقیقات بر روی روند سانسور در کشور، ما شاخص هایی را یافتیم مبنی بر این که می توانند به صورت عمدی یا غیر عمدی آدرس های راه دور را به صورت آدرس دهی درون کشوری هدایت کنند. این بدان معنی است که یک شبکه خصوصی تنها برای دسترسی درون کشوری وجود دارد. علاوه بر این، بر اساس اطلاعات جمع آوری شده از "سامانه نام دامنه ها" (DNS) نشان می دهد که برخی دسترسی ها با استفاده از سیستم 'dual stack' (استفاده هم زمان از IPv4 و IPv6) فعال هستند. در این حالت سرویس دهنده ها علاوه بر IP که در داخل کشور به آن ها اختصاص داده شده، از یک IP مجزا برای دسترسی جهانی استفاده می کنند. با وجود پیامدهای سیاسی مشخصی که این ادعا در پی خواهد داشت و به ویژه بر اساس ماده 46 "برنامه پنج ساله پنجم توسعه" برای توسعه شبکه ملی اطلاعات، می توان به قصد و منظور این روش پی برد. بر همین اساس و برای به دست آوردن بازخوردی مناسب در تحقیقات آینده، همین طور برای این که نشان دهیم که این موضوع نیازمند توجه گسترده تر جامعه جهانی است اطلاعات به دست آمده در این تحقیقات را منتشر می کنیم.

کلمات کلیدی: سانسور، اینترنت ملی، ایران، rfc1918

1- مقدمه

هدف اولیه این مقاله، مستند کردن این واقعیت است که ایران قوانین آدرس دهی استاندارد معمولی در اینترنت را نقض کرده تا یک شبکه خصوصی ایجاد کند که تنها از داخل کشور در دسترس است. تلاش اولیه ما در جهت این است که نشان دهیم که این شبکه داخلی قابلیت دسترسی به تعداد زیادی از کاربران داخلی را دارد. پس از آن شروع به طرح یافته های خود برای دامن زدن به این بحث و همین طور درخواست بازخورد در رابطه با این ادعا می کنیم. این مقاله باید به عنوان مقدمه ای برای مطالعه گسترده تر ساختار ارتباطات، زیرساخت اطلاعات در ایران و رژیم سانسور در نظر گرفته شود و به عنوان مثال راهی باشد برای این که در آینده و زمان مناسب پرسش های بزرگتری در مورد این موضوعات مطرح شود. علاوه بر این، تا حد امکان، ارزیابی های ما بر آنچه از لحاظ کیفی قابل اندازه گیری است متمرکز شده و تلاش شده است که پیش بینی مسائلی که جنبه سیاسی دارند تا حد امکان محدود شوند. ما این مقاله را جامع در نظر نمی گیریم و ممکن است با وجود دقت دچار اشتباه شده باشیم.

براساس این اهداف، طرح ما بر این سه اصل استوار است:

1. ما نشان می دهیم که یک تصمیم هماهنگ شده توسط زیر مجموعه ای از شرکت های ارائه خدمات اینترنتی ایرانی (ISP) و سازمان های دولتی برای استفاده از پروتکل اینترنت خصوصی (IP) در آدرس دهی در شبکه ها وجود دارد.
2. ما شروع می کنیم به شناسایی مشارکت کنندگان در این چیدمان و نقشه محله های منطقی در فضای خصوصی.
3. ما تلاش می کنیم تا خدمات و منابعی که در این شبکه مخفی در دسترس است را برشماریم.

اکثر آزمایشات مشخص شده ما را به سمت جمع آوری اولیه انگیزه از داده های بی پایان در یک پدیده غیرمنتظره سوق می دهند، که نتایج آن برای دسترسی عموم و بررسی بیشتر در آدرس زیر در دسترس است:

http://github.com/collina/filternet

مقاله به شکلی که توضیح داده می شود پی ریزی شده است. در بخش 3، ما همه روش های موجود را برای استخراج اطلاعات از منابع مختلف جهت دستیابی به طبیعت شبکه استفاده می کنیم. اصول اساسی آدرس دهی استاندارد در شبکه در بخش 2 به طور

[1] English version: https://arxiv.org/abs/1209.6398

خلاصه بحث می شود، این اطلاعات سپس در رابطه با ایران در بخش 4 به کار گرفته می شوند. در بخش 4.1، تلاش ما بر این است که نشان دهیم دسترسی به شبکه یک پدیده محلی نیست و شواهدی ارائه دهیم که نشان دهیم این ویژگی محصول طراحی عمدی است. روش های جمع آوری داده ها مورد استفاده برای توصیف محتوا بر روی شبکه در بخش 5 بحث شده است. و در نهایت، مقاله با برشمردن تعدادی سوالات پاسخ داده نشده در بخش6 به نتیجه گیری می رسد.

1.1 توضیحی در رابطه با نحوه بیان

ادعاهای مطرح شده در این مقاله همراستا با نگرانی در رابطه با آینده اینترنت ایران مطرح شده است، به خصوص نگرانی در رابطه با این که دولت از یک استراتژی تهاجمی برای فیلترینگ به مسدود کردن دسترسی به تمام سایت های خارجی تغییر رویه بدهد. ما می دانیم که در سند چشم انداز پنجم پنج ساله توسعه جمهوری اسلامی (2010 تا 2015) توسعه شبکه ملی اطلاعات جهت مقاصدی مانند: خدمات دولت الکترونیک، صنعت، فن آوری اطلاعات، سواد اطلاعاتی، افزایش بهره وری در حوزه های اقتصادی و فعالیت های اجتماعی فرهنگی در نظر گرفته شده است. در ادامه این طرح به توصیف نیاز به ارتباطات امن و خصوصی بین وزارت خانه های دولتی، شرکت های تجاری و مردم، مبنی بر افزایش پهنای باند و سرمایه گذاری در مراکز داده ملی پرداخته شده است. پس از تدوین برنامه توسعه، رضا تقی پور، وزیر ارتباطات و فن آوری اطلاعات و دیگر مسئولان دولتی در اقدامی هماهنگ شروع به ستایش فضایل اینترنت ملی کرده و وعده جایگزین داخلی برای ایمیل و موتور جست و جو دادند در حالی که در رابطه با خطرات استفاده از خدمات خارجی سخن می گفتند.

علی آقامحمدی، معاون نظارت و هماهنگي در سياست‌هاي اقتصادي معاون اول رييس‌جمهوري در دولت محمود احمدی نژاد: «*یک شبکه واقعا حلال، با هدف مسلمانان در همه سطوح اخلاقی و معنوی*»

اسماعیل احمدی مقدم، فرمانده نیروی انتظامی جمهوری اسلامی: «*اینترنت ملی می تواند تاثیر به سزایی در حفظ اطلاعات کشور و امنیت مردم داشته باشد*»

در حالی که بخش قابل توجهی از این روایات در نشریات خارجی و وبلاگ های فارسی زبان به بدترین سناریوهای ممکن می پرداختند، تشابه نظرات رسمی و غیر رسمی، حاکی از یک شبکه داخلی تمام عیار داشت. هرچند، پس از تحقیقات، ما گزارش هایی از استفاده از آدرس های ملی خصوصی از ژانویه 2010 یافتیم. در آن زمان مرکز آمار ایران از مردم خواست تا از طریق سایت amar.org.ir اطلاعات خود مانند میزان درآمد و اموالشان را گزارش دهند. پس از آن گزارش شد که دامنه بر روی آی پی 10.10.33.40 قرار دارد و بیش از 2 میلیون بازدید را ثبت کرده است. علاوه بر این، پر بازدیدترین صفحه ایرانی، یعنی صفحه سایت فیلترینگ بر روی آی پی داخلی 10.10.34.34 از تاریخ 23 ژوئیه 2010 فعال است. بنابراین، ادعای ما در این جا نه تازگی دارد و نه به نظر می رسد که حکومت برنامه ای برای قطع یک باره اینترنت جهانی در نظر گرفته است.

2- استانداردها در آدرس دهی خصوصی اینترنت

مبنای اساسی ارتباطات شبکه، انتساب منحصر به فرد IP آدرس ها در گروه هایی است که به عنوان زیر شبکه به میزبان شبکه به صورت منطقی تقسیم بندی شده اند. در سطح جهانی، نیاز است که شماره های منحصر به فرد شبکه، مانند IP یا شماره های مستقل سیستم(ASN)[2] اعتبار مرکزی برای تخصیص و هماهنگی داشته باشند تا از اختلال[3] جلوگیری شود. این مسئولیت بر عهده یک بخشی از سازمانی خصوصی به نام IANA[4] و نمایندگان منطقه ای آن است. IANA مشخص می کند که هر شرکت ارائه خدمات اینترنتی (ISP) و اشخاص دیگر از چه بلوک های آدرسی استفاده کنند.

هرچند، از آنجایی که طرح آی پی های 32 بیتی محدود است و هر میزبان نیاز به دسترسی دو طرفه مستقیم به اینترنت ندارد، IANA سه بلاک از آدرس های IP را برای شبکه های محلی بدون نیاز به تایید و هماهنگی آزاد گذاشته است. براساس سند استانداردهای استفاده از آدرس های خصوصی، رختر[5] و همکارانش تفاوت میزبان عمومی و خصوصی را این گونه شرح می دهند:

---

[2] Autonomous Systems numbers

[3] conflicts

[4] the Internet Assigned Numbers Authority

[5] Rekhter یاکو رختر، یکی از شناخته شده ترین طراحان پروتکل های شبکه است. وی نقش به سزایی در توسعه پروتکل های اینترنتی از ابتدای شکل گیری اینترنت داشته است.

میزبان خصوصی، میزبانی است که قابلیت و نیاز دسترسی به اینترنت جهانی را ندارد و یا تنها نیاز به مجموعه ای محدود از خدمات خارجی دارد که می تواند توسط دروازه واسطه[6] گرفته شود. میزبان خصوصی بر همین اساس می تواند از IP هایی که در شبکه خصوصی ابهامی ایجاد نمی کنند (تشابهی ندارند) و در سطح اینترنت جهانی مبهم هستند (مشابه آن ها وجود دارد) استفاده کند.

میزبان عمومی، میزبانی است که نیاز به دسترسی خارج از محدوده شبکه خصوصی و حفظ IP مشخص دارد که در سطح جهانی بدون ابهام (انحصاری و بدون مشابه) باشد و منطقا قابل دسترسی به آن وجود داشته باشد.

تصویر شماره 1، لیست منفک شده ای از بلوک های قابل استفاده مجدد از IP ها را نشان می دهد که برای کمک جهت حفاظت از مجموعه ی محدود آدرس های جهانی در نظر گرفته شده اند تا استفاده از میزبان شبکه های کوچک تر و محلی را آسان کنند.

10.0.0.0 - 10.255.255.255	(آدرس 16777216)
172.16.0.0 - 172.31.255.255	(آدرس 1048567)
192.168.0.0 - 192.168.255.255	(آدرس 65536)

تصویر شماره 1: بلوک های IP های رزرو شده توسط IANA برای شبکه های خصوصی

کسانی که میزبان IP های اختصاص داده شده در یک بلوک آدرس های خصوصی هستند ممکن است در همان شبکه با یکدیگر در ارتباط باشند، با این حال، به طور مستقیم با شبکه گسترده تر و اینترنت جهانی در ارتباط نیستند.[7] RFC1918 به صراحت و روشنی انتظارات و رابطه میان میزبان و آدرس های خصوصی را بیان می کند.

به دلیل این که آدرس های خصوصی معنای جهانی ندارند، مسیریابی اطلاعات در مورد شبکه های خصوصی باید بر روی لینک درون شبکه ای محلی انجام شود و نمی تواند به صورت گسترده و خارج از شبکه محلی مسیریابی شود، و بسته های اطلاعاتی با منبع خصوصی یا آدرس خصوصی نباید از طریق لینک های خارج شبکه محلی ارسال شوند. از روترها در شبکه هایی که از بلوک آدرس های خصوصی استفاده نمی کنند، به خصوصی ارائه دهندگان خدمات اینترنتی، انتظار می رود که به نحوی پیکربندی شده باشند که مسیریابی اطلاعات در مورد شبکه های خصوصی را فیلتر کنند. اگر چنین روترهایی، این چنین اطلاعاتی را دریافت و آن ها را فیلتر کنند، به عنوان یک خطای پروتکل لحاظ نمی شود.

شبکه های سنتی با استفاده از مکانیزم NAT[8] اجازه می دهند تا واسطه ها در سطح جهان به عنوان دروازه عمل کنند و به صورت شفاف به ارسال و دریافت ترافیک به اینترنت جهانی از طرف میزبان خصوصی در همان شبکه اقدام کنند. از آن جا که تعداد دستگاه هایی که به صورت مستقیم به اینترنت متصل می شوند افزایش یافته است، تعداد IP های تخصیص نیافته برای شبکه ها کاهش یافته و بسیاری از شرکت های ارائه خدمات اینترنتی از تکنیک هایی مانند Carrier-Grade NAT یا Large-Scale NAT[9] استفاده می کنند. همانند NAT در یک مجموعه، در شبکه CGN، تعدادی از کاربران محلی، یک آدرس عمومی را به اشتراک می گذارند، در حالی که هر کاربر یک آدرس خصوصی داخلی مجزا در شبکه را به خود اختصاص داده است. این طرح آدرس دهی

---

[6] intermediary gateways

[7] در معماری آدرس دهی اینترنت، شبکه خصوصی شبکه‌ای است که از آدرس‌های IP خصوصی استفاده می‌کند که در RFC1918 و RFC4193 آمده‌است. این آدرس‌ها عموماً برای شبکه‌های محلی خانگی، اداری و شرکتی زمانی که آدرس‌های جهانی قانونی نیستند یا برای برنامه‌های مخصوص شبکه در دسترس نمی‌باشند استفاده می‌شود. تحت IPV4 آدرس IP خصوصی در اصل در تلاش برای به تأخیر انداختن پر شدن IPV4 تعریف شدند اما همچنان یکی از ویژگی‌های IPV6 هم هستند. این آدرس‌ها به عنوان خصوصی بخش بندی می‌شوند زیرا آن‌ها بصورت جهانی تعیین نشده‌اند. یعنی این که آن‌ها به هیچ سازمان خاصی اختصاص ندارند و بسته‌هایی که با آن‌ها آدرس دهی شده‌اند نمی‌توانند به اینترنت راه یابند. هر کس می‌تواند بدون این که از یک سازمان ثبت اینترنت منطقه‌ای مجوز بگیرد از آن‌ها استفاده کند. اگر یک همچنین شبکه‌ای نیاز به وصل شدن به اینترنت داشته باشد. باید یا از NAT و یا از یک سرور بروکس استفاده کند.

[8] network address translation، برگردان نشانی شبکه، در شبکه‌بندی رایانه‌ای، روشی است برای فرستادن و دریافت ترافیک شبکه از طریق مسیریاب که با بازنویسی IP منبع و یا مقصد سروکار دارد و گاه نیز با شماره درگاه‌های TCP/UDP که بسته‌های IP از آن می‌گذرند، ارتباط دارد. می‌توان گفت اگر چند رایانه از راه LAN با هم پیوند دارند و هر یک نشانی IP محلی دارند و می‌خواهند از راه یک رایانه که به شبکه اینترنت پیوند دارد (WAN) و نشانی IP جهانی دارد از اینترنت بهره ببرند، در اینگاه از این روش بهره می‌برند.

[9] CGN یا LSN، رویکردی در طراحی شبکه IPv4 است برای سایت های نهایی در شبکه های شناخته شده خاص، همراه با آدرس های خصوصی است که توسط دستگاه های ترجمه middlebox اجازه اشتراک گذاری مجموعه کوچک تری از آدرس های عمومی را میان سایت های بیشتری فراهم می کند.

نیز به منظور محدود کردن دسترسی به محتوای منحصر به فرد مانند پروتکل تلویزیون اینترنتی[10] برای مصرف کننده و کاهش در معرض آسیب قرار گرفتن از سوی عوامل خارجی، قوی تر شده است.

3- راه اندازی آزمایشی

قبل از توصیف یافته های ما، نیاز است به جنبه های اخلاقی مختلف پژوهش انجام گرفته اشاره شود و پس آن به طرح روش که ما را قادر به انجام تجزیه و تحلیل کرده است بپردازیم. در نهایت ما این بخش را با پرداختن به کاستی های این رویکرد و پرداختن به چگونگی تلاش برای کاهش مشکلات بالقوه به پایان می بریم.

3.1 – جنبه های قانونی و اخلاقی

در فرآیند آماده سازی و اجرای آزمایش ها، توجه ویژه ای داشتیم که هیچ یک از قوانین را نقض نکنیم، و با توجه به احتمال کاهش برای همکاری های بین المللی یا آزادی بیان، افراد در ایران در معرض آسیب احتمالی قرار نگیرند. علاوه بر این، تمام آزمون های ما مطابق با هرگونه شرایط مربوط به خدمات و ملاحظات معقول از استفاده از شبکه بود تا به عنوان توده نفوذی از سوی شبکه ها تلقی نشویم. در بررسی ادبیات تحقیق علوم کامپیوتر، ما متوجه شدیم که نقشه برداری گسترده از شبکه های قابل دسترس به شیوه ای قابل قبول برای جمع آوری داده ها در رابطه با کیفیت تراکم اینترنت و زیرساخت شبکه تبدیل شده است. همزمان با این کار، جمع آوری داده های ما به عملکرد عادی و مورد انتظار از سیستم های از راه دور، که قابلیت دسترسی بدون نیاز به اعتبار را دارند، محدود شده است.

3.2 – نقاط مشاهده

برای اطمینان از این که یافته های ما یک پدیده محلی نیست، ما به دنبال به دست آوردن مجموعه ای ناهمگن از نقاط بهتری در بخش های منطقی ارتباطات زیرساخت ایران به منظور اندازه گیری و مشاهده بودیم.

میزبان شماره 1، تهران: بخش عمده ای از آزمایش های اولیه ما از میزبانی در تهران که ارائه دهنده میزبانی به سازمان های دولتی مانند صدا و سیمای جمهوری اسلامی است، انجام شد. در حالی که خارج از محدوده این مقاله، میزبان شماره 1، همکار بالادست اولیه راشن روستلکام[11] روسیه (AS12389) از طریق سازمان فن آوری اطلاعات (AS12880) است.

میزبان شماره 2، تهران: آزمایش دوم از یک شبکه دسترسی بالادست است که ارائه دهنده سرویس به چندین دانشگاه، وزارت بازرگانی و موسسات تحقیقاتی وابسته به وزارت علوم، تحقیقات و فن آوری است انجام گرفت. ارائه دهنده بالادست اولیه برای میزبان شماره دو، دلتا تلکام[12] (AS29049) از طریق موسسه پژوهش در علوم بنیادی (AS6736) است.

HTTP پروکسی های باز: به منظور انجام آزمون از بازه هرچه گسترده تری از زیر مجموعه شبکه های ایران، ما تعدادی از حوضچه های آشکارا در دسترس HTTP پروکسی، در هر دو آدرس های عمومی و خصوصی با درخواست از مجموعه ای مخلوط از میزبان های دولتی و خصوصی را در نظر گرفتیم. به منظور مقاصد محدود ما، فرض کردیم که اگر پروکسی قادر به رِلِه موفقت آمیز درخواست بود، برخی از سطوح اتصال میان واسطه و مقصد وجود دارد. بعد از اسکن عمومی از بلوک های IP های در دسترس ایران برای سِرورهایی که بر روی پورت های استفاده شده توسط خدمات کَش وب اسکوییید[13] در حال دریافت بازخوردها بودند، حدود صد پروکسی در 27 شبکه شناسایی شد. همین روند در فضای آدرس های خصوصی نیز تکرار شد و 15 پروکسی در شبکه های نامشخص را شناسایی کرد.

3.3 – کاستی ها

محدودیت های طبیعی در تحقیقات از یک مجموعه کوچک از میزبان ها توسط کشور تحمیل شده است، به ویژه در جاهایی که اطلاعات خارج از محدوده وجود دارد. علاوه بر این، باید توجه داشته باشیم که ما هیچ اطلاعات قابل اعتمادی در مورد صاحبان نقاط مورد مشاهده مانند این که آیا آنها محدود به فیلترهای محلی که در نقاط دیگر با توجه به نوع فن آوری و پیچیدگی متفاوت باشد،

---

[10] Internet Protocol Television- IPTV

[11] Russian Rostelecom

[12] Delta Telecom

[13] Squid web cache service، اسکوئید یک پروکسی سرور است که روی http و https و ftp عمل میکند و می‌تواند به عنوان کارساز کش (کش‌سرور) نیز به کار رود.

نداریم. تجزیه و تحلیل فعال از سیستم سانسور و شبکه ها اگر با مراقبت های ویژه صورت نگیرد، به سرعت جلب توجه می کند. با توجه به سابقه حمله به توانایی عمومی برای دسترسی امن به اینترنت جهانی، توانایی هماهنگ کردن منابع اطلاعات در زمان یکسان، یک منبع حیاتی است که ما به دنبال حفظ آن برای استفاده های آتی هستیم.

ما به کاستی های ذکر شده در بالا در رابطه با روش های تجربی واقف هستیم، و منابع خود را طبقه بندی کرده ایم در حالی که تلاش می کنیم بر ادعای محافظ کار بودن خود بمانیم.

4- تحلیل

شاخص های در دسترس بسیاری از استفاده های ملی از آدرس های خصوصی در ایران در ساختار فیلترینگ و راه های مسیریابی بین المللی نهفته است. ایران یکی از تهاجمی ترین ساختارهای فیلترینگ در جهان را داراست، مثل مسدود کردن طیف گسترده ای از محتوا مانند نظرات مخالف نظام سیاسی حاکم، نظرات مخالف مذهبی و هنجارهای اجتماعی. تلاش برای دیدن این نوع محتوا، به شیوه تغییر مسیر به یک سایت جهت ارائه پیشنهاد برای رجوع به محتوای مورد حمایت حکومت می انجامد. درحالی که کاربر به نظر می رسد بر روی سایتی که قصد دیدن آن را داشته است باقی می ماند، اما در واقع تغییر مسیری در چارچوب مسیریابی او را به سمت IP خصوصی 10.10.34.34 هدایت می کند. (در تصویر 4، نتیجه برای دیدن درخواست بازدید از سایت Facebook.com مشاهده می شود.)

تصویر 2

```
traceroute to facebook.com (69.63.181.12)
...Home Network...
2 91.99.***.***.parsonline.net [91.99.***.***]
3 10.220.1.2
4 2.180.2.1
5 217.219.64.115
6 78.38.245.6
7 78.38.245.5
8 78.38.244.242
9 78.38.244.241
10 10.10.53.61
...Traffic Exits Country...
```

تصویر 2: دستور Traceroute برای اینترنت عمومی

```
traceroute to 10.10.34.34 (10.10.34.34)
...Home Network...
2 81.12.48.89 (81.12.48.89)
3 10.9.27.1 (10.9.27.1)
4 10.30.153.253 (10.30.153.253)
5 217.218.190.26 (217.218.190.26)
6 78.38.119.30 (78.38.119.30)
7 78.38.119.210 (78.38.119.210)
8 195.146.33.29 (195.146.33.29)
9 10.10.34.34 (10.10.34.34)
```

تصویر 3: دستور Traceroute به یک محتوای فیلتر شده

این مکانیزم سانسور، یکی از محصولات تمرکز شبکه در شرکت مخابرات ایران(TCI) است. تمام ترافیک بین المللی باید از طریق یکی از شرکت های تابعه شرکت مخابرات ایران به نام شرکت فن آوری اطلاعات ایران (AS12880) یا مرکز تحقیقات فیزیک نظری و ریاضیات (AS6736) عبور کند. برای اکثر شبکه های مصرف کننده که از طریق شرکت مخابرات ایران به اینترنت متصل هستند، به نظر می رسد هاب نهایی قبل از خروج ترافیک از کشور توسط یکی از حداقل سه روتر اصلی Huawei Quidway NetEngine80E که از آدرس خصوصی در محدوده 10.10.53.0/24 استفاده می کنند، به کار گرفته می شود. (به تصویر 2 نگاه کنید)

```
<html ><head >< meta http - equiv =" Content - Type " content =" text / html ; charset
=windows -1256" > < title >F1 -IPM </ title ></ head ><body >< iframe src = http ://10.10.34.34?
type = Invalid Site & policy = MainPolicy " style =" width : 100%; height : 100%"scrolling =" no"
marginwidth ="0" marginheight ="0" frameborder ="0" vspace="0" hspace ="0" > </ iframe ></
body ></ html >
```

تصویر 4: پاسخ به درخواست فیلتر شده GET

در حالی که انتظار می رود بر اساس استاندارد برای زیرساخت های شبکه در زمانی که به دلایل امنیتی، انعطاف پذیری و منابع محدود، باید تحت قانون RFC1918 از آدرس های خصوصی استفاده شود، میزبان نباید از خارج از این شبکه ها توسط آن آدرس خصوصی قابل دسترس باشد. به منظور اندازه گیری حجم فضای این شبکه خصوصی که شرکت مخابرات ایران و دیگران از آن استفاده می کنند، ما اقدام به اتصال به تمام 16777216 آدرس امکان پذیر از بلوک 10.0.0.0/8 IP کردیم.

Service (Port)	Number of Host
FTP (21)	12672
SSH (22)	8029
Telnet (23)	20060
SMTP (25)	183
DNS (53)	2510
POP (110)	78
HTTP (80)	9960
IMAP (143)	44
HTTPS (443)	1366
HTTP-Alt (8080)	601

تصویر 5: خدمات بر روی فضای آی پی های خصوصی

داده های ما در سه فاز جمع آوری شد: پیدا کردن آدرس های IP که اتصال به پورت 23 TCP (TelNet)، پورت 53 (DNS) یا پورت 80 (HTTP) را می پذیرند؛ انجام دست دهی[14] ساده و ذخیره اطلاعات و نقشه برداری از روترها برای تعیین گروه بندی منطقی و مسیرها. با توجه به حوضچه شبکه های بالقوه، ما این محدوده را به 45928 میزبان بالقوه محدود کردیم.

4.1 – اندازه گیری میزان دسترسی به شبکه های خصوصی

همانطور که در بخش 3 اذعان شد، یافته های ما به طور طبیعی برای این که بتوانیم ادعا کنیم برای کل شبکه در داخل کشور معتبر هستند، محدود است. حتی براساس اظهارات عمومی مقامات وزارت ارتباطات و فن آوری اطلاعات، اجرای ماده 46 همچنان ناقص است و اولویت بندی با موسسات دانشگاهی و وزارت خانه هاست. بنابراین، ما انتظار نداریم که دسترسی جهانی در تمام مناطق جغرافیایی و یا تمام شبکه ها با این یافته ها سازگار باشد.

ما با استفاده از حوضچه باز پروکسی های در دسترس جهانی، اقدام به درخواست پروکسی HTTP GET از موارد زیر کردیم: 1) یک وبسایت با دسترسی جهانی که در داخل کشور قرار داشته باشد، 2) یک دامنه که به یک آدرس IP خصوصی متصل باشد، 3) یک IP خصوصی که خدمات وب ارائه دهد و 4) یک وبسایت خارجی که در داخل کشور فیلتر نباشد، برای اطمینان از این که پروکسی درست کار می کند. اگر هر کدام از این درخواست ها با پاسخ "OK 200" بازگشت کنند، که پاسخ استاندارد برای

[14] Handshake، در هر اتصال رایانه‌ای مقداری بار اضافی وجود دارد که در اصطلاح دست‌دهی نامیده می‌شود و بدین معنی است که مودم از کامپیوتر سرور سوال می‌کند، آیا داده‌ها را دریافت کرده است و سرور پاسخ مثبت یا منفی می‌دهد.

درخواست HTTP است و با عنوان صفحه مورد درخواست ما مطابقت داشته باشند، آنگاه مقصد نهایی در دسترس قلمداد می شود. به موازات این مورد، این آزمایش با مجموعه ما از آدرس های خصوصی نیز تکرار شد. با استفاده از این فرآیند، ما می توانیم بررسی کنیم که 27 شبکه مجزا و 12 میزبان با آدرس خصوصی، قادر به رسیدن به حداقل یک میزبان از فضای خصوصی ما بوده اند. با تکیه بر سِرورهای پروکسی برای اندازه گیری اتصال به شبکه های خصوصی به تعدادی از سناریوهای فرضی که به دلیل پیکربندی اشتباه در بخش مدیریت و یا محدودیت در استفاده در نظر گرفته شده اند، ممکن است باعث ایجاد منفی کاذب شوند. مثبت کاذب نیز ممکن است رخ دهد، هرچند، شرایطی که ممکن است تحت آن مثبت کاذب رخ دهد قابل پیش بینی است و از آنجایی که ما یکپارچگی نتایج به دست آمده را با نتایج مورد انتظار مطابقت می دهیم، به نظر می رسد این اتفاق کمتر محتمل است. بنابراین، ما توجه خود را بیشتر به ارتباطات موفق به عنوان اندازه گیری اتصال منعطف می کنیم و به ارتباطات ناموفق توجه زیادی نمی کنیم.

نتایج این اندازه گیری ها در لیست شماره 9 آورده شده است. از شبکه های عمومی در دسترس 24 مورد (89%) حداقل یک میزبان که به IP های خصوصی Iran.ir متصل بوده است داشته اند و 21 مورد (77%) قادر به اتصال به دانشگاه بین المللی امام رضا بوده اند. برای پروکسی های داخلی نیز، 13 مورد قادر به اتصال به Iran.ir و 6 مورد قادر به دسترسی به دانشگاه بوده اند.

5- شبکه های خصوصی تا چه حدی گسترده و مورد استفاده هستند

بر خلاف اینترنت جهانی، هیچ ثبت عمومی برای شبکه های متصل به فضای آدرس های خصوصی وجود ندارد. بنابراین، ما به دنبال یک روش ترکیبی از استخراج متن باز[15] برای شروع یک نقشه بسیار اولیه از اینترنت پنهان هستیم. از طریق روش جمع آوری داده ها، مانند جمع آوری آگهی خدمات و ردیابی مسیر ترافیک، ما قادر به شناسایی اطلاعات عمومی میزبان ها با آدرس خصوصی بودیم، که به شرح زیر است: 1) محل های منطقی شبکه ها، 2)استفاده هدفمند از شبکه های خصوصی و 3) هماهنگی گسترده در زیرساخت های شبکه. تعداد قابل توجهی از پاسخ ها شامل FQDN[16] و آدرس های عمومی بود که می تواند به صورت همسان در مقابل اطلاعات ثبت شده عمومی قرار بگیرد. با استفاده از این روش، ما شروع به ساختن درک ابتدایی از مالکیت منطقی و شرکت در شبکه ملی به دست می آوریم که در تصاویر شماره 7 و 8 آورده شده است.

5.1- سر صفحه خدمات

در طول شماره گذاری میزبان های مشخص شده در بخش 4، ما به دنبال شناسایی خدمات اطلاع رسانی اینترنتی به خصوص وب، ایمیل و سرویس دهنده های دامنه ای بودیم که در فضای شبکه های خصوصی هستند. پس از شناسایی از میان 16777216 آدرس IP که توسط میزبان ها اشغال شده بودند، سپس ما قادر به ارزیابی ثانویه از داده ها و تلاش برای ارزیابی مقدار محتوای وب که به فضای خصوصی آدرس دهی شده بودند شدیم.

```
$ nc 10.143.177.18 25
220 webmail.isfidc.com ESMTP
MailEnable...
$ dig +short webmail.isfidc.com
91.222.196.18
```

تصویر 6: بنر گرفتن در SMTP

با توجه به مقیاس این چنین جست و جویی، تعیین این که یک سرویس خاص در دسترس باشد، بر پایه یک تصدیق ساده توسط یک میزبان از راه دور ممکن بود که برخی برنامه ها با پورت باز به سمت آن میزبان در ارتباط باشند. بسته به نوع خدمات ارائه شده توسط آن وب، تعدادی از متغیرها می توانند ما را به سمت نتایجی که با واقعیت موثر مطابقت داشته باشند منحرف سازند. به عنوان مثال، بسیاری از روترهای DSL خانگی به پیکربندی دستگاه اجازه می دهند تا از طریق یک وب یا یک شبکه راه دور به عنوان

---

[15] Open source

[16] FQDN، fully qualified domain name یک نام دامنه است که محل دقیق قرار گیری آن در DNS مشخص است.

front end[17] استفاده شوند، که تفکیک تفاوت آن از یک سایت کامل اینترنتی سخت خواهد بود. علاوه بر این، شرکت ها عموما میزبان چند وب سایت بر روی یک سِرور هستند، که یک ارتباط ساده مقدار اطلاعات موجود را فاش نمی سازد. با در نظر داشتن این نکته، تصویر شماره 5، جزییات نتایج حاصل از این جست و جو را نمایش می دهد.

همانطور که گفته شد، در حالی که مالکیت بخش هایی از IP از جمله اطلاعات عمومی است، چنین اطلاعاتی در رابطه با آدرس های خصوصی وجود ندارد. به هر صورت، این چنین اسکن هایی نمایش دقیقی از غنای محیط به دست می دهد، اکتشاف مالکیت منطقی زیر مجموعه ها را با ایجاد ارتباط میزبان در شبکه ها با سازمان های خاص یا بلاک شبکه های عمومی، تسهیل می کند. همانطور که در تصویر 6 نشان داده شده است، بسیاری از خدمات هویت خود را تنها با ایجاد یک اتصال ساده با آن ها به سادگی فاش می سازند. اطلاعاتی مانند FQDN می توانند به یک IP عمومی متصل شوند، این لینک سپس می تواند با مطابقت اطلاعات ثانویه مانند برچسب زمانی نسخه های نرم افزاری دارای اعتبار شود. پس از آن که اطمینان حاصل شد که IP های 10.143.177.18 و 91.222.196.18 به احتمال زیاد سرورهای همسان هستند، ما می توانیم به صورت منطقی فرض کنیم که برخی از زیرشبکه ها که حاوی آدرس 10.143.177.18 باشند، متعلق به مرکز تحقیقات کامپیوتری حوزه علمیه اصفهان هستند. حتی در جایی که اطلاعات بازیابی شده ناقص است، حاوی زمینه ای در رابطه با محل یا اطلاعات محدودی در رابطه با احتمالات برای تحقیقات بیشتر مانند تطبیق محتوای پاسخ سِرور وب خصوصی با سایت هایی که اجزای عمومی آن توسط Web Crawler[18] موتورهای جست و جو ثبت می شود را فراهم می کند. ما هم چنین ممکن است شاخص هایی برای تعیین این که اکثریت لینک ها به سایت ها از کجا بازگشت می کنند پیدا کنیم.

5.2- سوابق DNS

یکی از جنبه های به خصوص قابل توجه از یافته های ما، رخ دادهای دامنه است که سوابق DNS را معتبر نگاه می دارد، مانند آدرس های IP خصوصی در دسترس و یا سوابق چندگانه که شامل اطلاعات هر دو بخش عمومی و خصوصی است. ارزیابی از تمام سوابق DNS دشوار است چرا که IRNIC که نگهدارنده[19] بالادست دامنه ایران (.ir) است، به نظر نمی رسد تمایلی به انتشار فایل های منطقه ای که شامل لیست دامنه های ثبت شده در آن است، داشته باشد. بنابراین اطلاعات ما به بررسی منابع عمومی و سرصفحه های خدمات برای ساخت تصویر شماره 8 محدود شده است.

5.3 – پیمایش NAT و انحراف ICMP[20]

برای برقراری ارتباط دو طرفه جهت دسترسی به ماشین های اینترنتی که دارای آدرس اختصاصی هستند یا باید یک آدرس اضافی عمومی داشته باشند یا قادر به انتقال اطلاعات از طریق یک درگاه NAT. از آنجا که ما تا حد زیادی علاقمند به دسترسی جهانی و همچنین ارتباط خصوصی با آدرس های عمومی هستیم، اما قادر به پرس و جو مستقیم از میزبان های فضای خصوصی نیستیم، تلاش می کنیم که یک درخواست ICMP Echo[21] از درون کشور به یکی از آدرس های خصوصی از طریق جعل آدرس منبع به عنوان این که ما یک سرور خارج از کشور هستیم بدهیم. مقصد باید یک پاسخ پینگ[22] به میزبان خارجی ارسال کند. اگر پاسخ از یک درگاه در طول مسیر خود عبور کند، آدرس خصوصی از میزبان از راه‌دور با آدرس های عمومی واسطه ها بازنویسی خواهد شد تا شواهدی از مالکیت شبکه را به دست دهد. درخواست ICMP Echo با استفاده از زمینه توالی داده ها به جهت مرتبط کردن

---

[17] Front end در علم کامپیوتر مسئولیت جمع آوری اطلاعات از ورودی های مختلف و پردازش آن به طوری که برای back end قابل فهم باشد را دارد.

[18] Web Crawler، یک برنامه‌ای رایانه‌ای است که توانایی مرور و ثبت اطلاعات را از وب‌سایت‌ها به صورت خودکار دارد. "خزنده‌ی وب" به چندین شکل مختلف تعریف می‌شود که برخی از آنان عبارتند از Automatic Indexers، Web Robots، web spider. یکی از موارد استفاده از این نرم افزارها در موتورهای جست و جو است، موتورهای جستجوگر با بهره‌گیری از این گونه نرم‌افزارها به صورت خودکار صفحات مختلف وب سایت‌ها را ثبت ، آنالیز و رده‌بندی می‌کنند

[19] Maintainer، Holder

[20] Internet Control Message Protocol، پروتکل کنترل پیام‌های اینترنتی یکی از پروتکل‌های اصلی بستهٔ پروتکل‌های اینترنت است. مورد اصلی استفاده از آن در سیستم عامل های کامپیوترهای متصل به شبکه، برای ارسال پیام‌های خطا مانند سرویس مورد درخواست در دسترس نیست و یا ارسال پیام در رابطه با میزبان یا روتر غیرفعال، است. از آی‌سی‌ام‌پی می توان برای رله کردن دستورها نیز استفاده کرد.

[21] ICMP Echo یا Ping یک ابزار شبکه‌ای است که برای آزمایش میزان دسترسی‌پذیری یک میزبان در شبکهٔ پروتکل اینترنت به کار می‌رود و می‌تواند زمان رفت و برگشت برای بسته‌های فرستادهشده از میزبان عامل تا یک رایانهٔ مقصد را محاسبه کند.

[22] ping، ICMP Echo-Reply به وسیله فرستادن یک بسته درخواست انعکاس با استاندارد ICMP به هدف منتظر ماندن برای گرفتن پاسخ از نوع ICMP عمل می‌کند. در این فرایند زمان رفت و برگشت محاسبه می‌شود و هر گونه از دست دادن بسته ثبت می‌شود. در آخر نتیجه چاپ شده از این فرآیند، جمع‌بندی‌های آماری از پاسخ بسته‌های رسیده شامل بیشترین، کمترین، میانگین زمان رفت و برگشت بسته‌ها و گاهی انحراف معیار از این میانگین خواهد بود.

پرسش آدرس های خصوصی با پاسخ های مشاهده شده، به تمام میزبان های از راه دوری که قبلا شناسایی شدند ارسال شد. دلایل متعددی برای این که یک میزبان به ICMP Echo پاسخ ندهد وجود دارد که از آن جمله می توان به تنظیمات دیواره آتش[23] و یا تغییر در قابلیت دسترسی از طریق اسکن اشاره کرد. از میان 45928 میزبانی که از آن ها پرسش صورت گرفت، 10344 مورد پاسخ دادند که در این میان 358 مورد از آن ها آدرس منبع عمومی داشتند. 408 مورد با آدرس های خصوصی دیگری نسبت به آن آدرسی که از آن ها پرسیده شده بود پاسخ دادند که می تواند به دلایلی مانند پاسخ از سوی یکی از واسطه ها در طول مسیر بوده باشد یا میزبان راه دور به چندین آدرس متصل باشد. باقی پاسخ ها حاوی آدرس خصوصی بود که از آن پرسش شده بود. اکثریت قریب به اتفاق آدرس های عمومی دیده شده به شبکه شرکت فن آوری اطلاعات شرکت مخابرات ایران تعلق دارند و باقی آن ها متعلق به آسیاتک (2 میزبان)، شرکت سروش رسانه (8 میزبان)، 1) CallWithMe میزبان) و ندا رایانه (6 میزبان) هستند.

5.4- ردیابی مسیر داده

ردیابی مسیر شبکه جزیی است و شواهدی از طرح آدرس دهی خصوصی به دست می دهد. با استفاده از نمونه ای از صفحه سایت فیلترینگ (10.10.34.34)، تصویر شماره 3 مسیری که یک درخواست طی می کند تا به مقصد خود برسد را نشان می دهد. توجه داشته باشید که آدرس IP بلافاصله قبل از مقصد نهایی (195.146.33.29) به نام مرکز امور ارتباطات داده ها که زیر مجموعه فناوری ارتباطات محسوب می شود، ثبت شده است. از آنجا که ترافیک شبکه از طریق مرکز داده ها مسیریابی می شود که میزبان آن قبل از رسیدن به مقصد نهایی قرار گرفته است، می توانیم نتیجه بگیریم که مرکز امور ارتباطات داده ها نقش مهمی در حفظ و نگهداری دستگاه های فیلترینگ بر عهده دارد. ما می توانیم همین نظریه را به مقصدهای مجزایی از شبکه که مسیریابی آن به آدرس های IP که با 10 شروع و به 1 ختم می شوند، با این فرض که آن ها نشان دهنده کوچکترین تقسیم بندی منطقی از فضای آدرس های خصوصی است، تعمیم دهیم. با استفاده از میزبان های درون کشوری، قادر به ترسیم نقشه های مسیر در تصاویر شماره 12 و 13 هستیم. ما این کار را با استخراج آدرس های عمومی منحصر به فرد موجود در مسیریابی و تعیین مالکیت آن ها در تصویر شماره 10 انجام داده ایم.

IP Address	Host/Network
10.8.12.18	Iran.ir National Webmail Service
10.8.218.0/24	Pishgaman, ADSL Internet Service Provider
10.10.34.34	Data Communication Affairs's Filtered Site Page
10.10.36.0/24	Telecommunications Company of Iran
10.30.54.0/24	Parsonline, ADSL Internet Service Provider
10.254.50.0/24	Islamic Republic of Iran Broadcasting
10.9.28.0/24	Islamic Republic of Iran Broadcasting
10.143.218.199	Telecommunications Company of Isfahan
10.56.59.198	Khorasgan Islamic Azad University, Isfahan
10.7.234.0/24	Ministry of Agriculture
10.30.170.0/24	Ministry Of Education
10.21.243.37	National Internet Development Agency of Iran

تصویر 7: نمونه هایی از شبکه ها و سایت های قابل شناسایی بر روی فضای شبکه خصوصی

6- نتایج و سوالات بیشتر

ما به دنبال روشن کردن و جمع آوری اطلاعات یکی از جنبه های قبلا ناشناخته و غیر معمول زیرساخت اطلاعات و فن آوری اتباطات ایران بودیم و پس از آن شواهدی به دست آمد که طراحی شبکه مورد اشاره طراحی هدفمندی را توصیف می کند. از طریق تجزیه و تحلیل مقایسه ای منابع گوناگون، ما باید شواهد و مدارکی برای این فرض خود به دست بیاوریم که اینترنت ملی در داخل در حال شکل گیری و به طور گسترده در دسترس است. علاوه بر این، درحالی که ما تلاش نمی کنیم درباره آینده ارتباط بین المللی ایران پیش بینی انجام دهیم، حدس می زنیم که اینترنت در جمهوری اسلامی هر روز بیشتر به خودمختاری هسته مرکزی قدرت نزدیک می شود. در این شرایط، فضای شبکه های خصوصی که ما با آن ها مواجه شدیم، به سمت انتظارات وزارت ارتباطات و

[23] Firewall، نام عمومی برنامه‌هایی است که از دستیابی غیر مجاز به یک سیستم رایانه جلوگیری می‌کنند. در برخی از این نرم‌افزارها، برنامه‌ها بدون اخذ مجوز قادر نخواهند بود از یک رایانه برای سایر رایانه‌ها، داده ارسال کنند.

فن آوری اطلاعات در حال پیشروی هستند. هرچند، ما در حرکت رو به جلوی خود، بیش از پاسخ، سوال مطرح کرده ایم، از این رو نیاز به پاسخ فوری برخی پرسش ها که در ادامه می آید را ضروری می دانیم:

- **آیا طرح آدرس های خصوصی به ناکارآمد شدن IPv4 ارتباطی دارد؟**

براساس اطلاعات RIPE که اطلاعات آدرس های IPv4 تا 18 سپتامبر 2012 را بازیابی کرده است، به شبکه های ثبت شده در ایران تقریبا 9555968 آدرس IPv4 اختصاص داده شده است. درحالی که با توجه به تعداد خانه هایی که به اینترنت متصل هستند، به نظر نمی رسد ایران به نقطه ای نزدیک شده باشد که IPv4 در آن ناکارآمد شده باشد. با توجه به گروه دستگاه های مصرف کننده با ظرفیت داده ها، همچنان سخت به نظر می رسد که نیازی به استفاده از راه حل هایی مانند CGN وجود داشته باشد. هرچند سناریوی مطرح شده در اینجا تفاوت اساسی با سناریو CGN برای مسیریابی خارج از شبکه های محلی دارد. علاوه بر این، CGN به صورت عمومی برای کاهش فشار از روی شبکه های خانگی و موبایل مورد استفاده قرار می گیرد، نه برای وزارت خانه های دولتی، دانشگاه ها یا میزبان محتوا.

- **آیا شبکه خصوصی امکان دسترسی به اینترنت جهانی را دارد؟**

در بخش 5.3، ما اقدام به آزمایش دسترسی عمومی فضای میزبان های خصوصی با جعل درخواست ICMP Echo به میزبان خارج از کشور کردیم. علاوه بر این، شبیه به چینش مورد استفاده در بخش 3.2، قدرت ارتباط گیری پروکسی ها به شبکه های خصوصی مورد آزمایش قرار گرفت. در هر دو مورد، ظاهرا تعداد کمی از سیستم هایی که از آن ها پرسش صورت گرفت، قادر به ارتباط از طریق درگاه NAT یا یکی از آدرس های اضافی که به میزبان متصل بود، هستند.

- **آیا ایران با استفاده از DNS سعی در جداکردن اینترنت ملی از ترافیک جهانی می کند؟**

همانطور که ما نشان دادیم، سازمان های ایرانی با کمی ابهام از سیستم دامنه برای پیاده سازی سایت های اینترنت ملی استفاده کرده اند. علاوه بر این، برخی موارد کمک دهنده هایی وجود داشته اند که به سایت ها اجازه می دادند از شبکه عمومی به شبکه خصوصی بروند. گام منطقی بعدی برای وجود ارتباطات راه دور، دستکاری در اجرای DNS یا مکانیزم تقسیم افق[24] در DNS برای دریافت پاسخ های مختلف از DNS براساس این که سرچشمه درخواست از داخل ایران یا خارج از کشور است خواهد بود. در تست های اولیه، ما شواهد کمی یافتیم که نشان می دهد ایران تلاش کرده است در عملیات DNS تداخل ایجاد کند؛ در عوض، فیلتر کردن سرویس های مختلف از قبیل HTTP به نظر می رسد از طریق ترنسپرنت پروکسی[25] و دیگر راه های ایجاد اشکال در رهگیری ترافیک صورت گرفته است. در روند بررسی محتوا در شبکه های خصوصی، ما تعدادی از FQDNها را یافتیم که به درخواست ها بی توجه بودند و توسط DNS ها به IP رهنمون نمی شدند. بعدها ما متوجه شدیم که همانطور که در تصویر شماره 11 نمایش داده شده است، یک مجموعه انتخاب شده ای از دامنه ها، مانند سرویس های عمومی IRNIC از DNS های ایرانی به درستی عبور می کنند. بازنگری در این موضوع نشان داد که زیرمجموعه های دامنه "Blizz.ir" تنها نمونه از این پدیده نیستند و نمونه های دیگری از دامنه ها مانند "isftak.ir" و "geeges.co.ir" نیز از همین قاعده پیروی می کنند. استفاده از آدرس های خصوصی برای DNS در Name-Server ها، هرچند عمدی یا غیر عمدی باشد، پتانسیل بالایی برای تداخل در عملیات های عادی اینترنت از طریق جلوگیری از گسترش جهانی مسیر اطلاعات دارد.

- **آیا فضای آدرس های خصوصی در حال رشد است؟**

داده های به دست آمده توسط این پروژه، دریچه ای باریک از مشاهدات در اواخر ماه آگوست و اوایل سپتامبر 2012 را نشان می دهد، بنابراین ما فاقد چشم انداز کافی برای بررسی این هستیم که آیا فضا در حال گسترش است یا فضای آدرس های عمومی در حال محدود شدن هستند. ما در بخش 1.1 نیز گفتیم که فضای آدرس های خصوصی از سال 2010 در حال استفاده است. بررسی چنین بلوک بزرگی از آدرس ها نیاز به تلاش قابل توجهی دارد و ممکن است توجه های غیر ضروری را به سمت ما جلب کند، بنابراین، پیشنهاد ما ادامه نظارت بر مسیرهای شبکه های معقول کوچک تری مانند کلاس C[26] است و بررسی های گسترده تر را به وقت مناسب موکول می کنیم.

---

[24] split-horizon

[25] transparent proxy،

[26] Class C یکی از گروه های IP های عمومی است که نیازی به ثبت توسط IANA ندارد. این گروه از IP ها به شکل X.Y.192.168 است.

- **چه مقدار محتوا به صورت انحصاری در شبکه خصوصی وجود دارد؟**

ما تلاش کردیم تا نشان دهیم که طیف گسترده ای از خدمات عمومی در شبکه خصوصی تکرار شده یا صرفا برای کاربران داخلی محدود شده است. این مورد براساس تحقیقات وقت گیر از نکات بازگشته از میزبان ها به دست آمده است و به هیچ وجه یک ارزیابی کامل از وضعیت شبکه ملی نیست.

تشکر و قدردانی

این تحقیق میسر نبود مگر با کمک افرادی که سهم قابل توجهی در انجام آن داشته اند و من افتخار آشنایی با آن ها را داشته ام، اما متاسفم که امکان نام بردن از آنها وجود ندارد. و باید گفت که تاثیر دلسرد کننده سانسور و تهدید دولت به مرزهای یک کشور محدود نمی شود. خوشبختانه امکان نام بردن از فابیو پیتروسانتی[27] و آرتور فیلاستو[28] وجود دارد که با بینش ارزشمند خود برای تحقیق کاربردی از شبکه به تکمیل این تحقیق کمک کردند.

ضمیمه

lib.atu.ac.ir	10.24.96.14	Allameh Tabatabaie University
www.mdhc.ir	10.30.5.163	Vice Presidency for Management Development and Human Capital
www.iranmardom.ir	10.30.5.148	Vice Presidency for Management Development and Human Capital
erp.msrt.ir	10.30.55.29	Ministry of Science, Research and Technology
ou.imamreza.ac.ir	10.56.51.27	Imam Reza University
www.tehranedu.ir	10.30.95.7	Tehran Education Organization
sanaad.ir	10.30.170.142	Private Individual
ww3.isaco.ir	10.21.201.50	Iran Khodro Spare Parts & After-sales Services Company
iiees.ac.ir	192.168.8.9	International Institute of Earthquake Engineering and Seismology
	169.254.78.139	
	194.227.17.14	
	10.10.3.2	
tci-khorasan.ir	217.219.65.5	Telecommunication Company of Iran, Khorasan
	10.1.2.0	
adsl.yazdtelecom.ir	10.144.0.14	Telecommunications Company of Iran, Yazd
iranhrc.ir	46.36.117.51	Private Individual
	10.30.74.3	
acc4.pishgaman.net	81.12.49.108	Pishgaman, ADSL Access Provider
	10.8.218.4	
lib.uma.ac.ir	10.116.2.5	University of Mohaghegh Ardabili
film.medu.ir	10.30.170.110	Ministry Of Education
www.shirazedc.co.ir	10.175.28.172	Shiraz Electric Distribution Company

تصویر 8: دامنه ها، مسئول سوابق و مالکیت آدرس های خصوصی

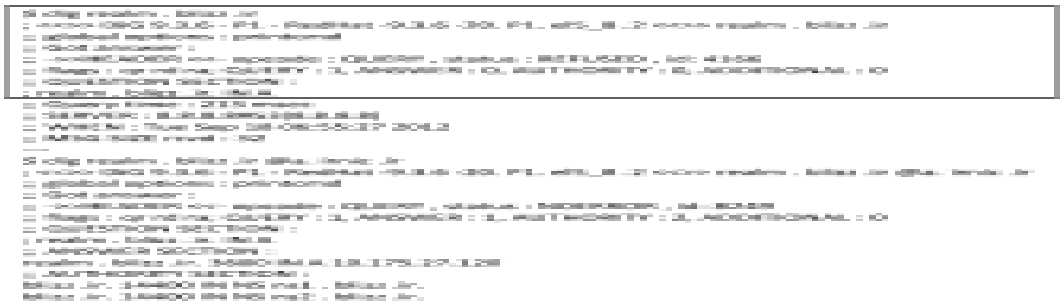
Fabio Pietrosanti [27]
Arturo Filasto [28]

ASN	(Hosts)	10.8.12.18	google.com	ou.imamreza.ac.ir	peyvandha.ir
RFC1918	(15)	13	9	6	12
44285	(2)	0	2	0	0
31549	(3)	0	0	1	0
50810	(2)	1	0	1	0
39501	(1)	1	1	1	1
48159	(4)	1	3	1	3
50892	(1)	1	1	1	1
42163	(2)	1	1	2	1
51235	(1)	1	1	1	1
16322	(5)	5	3	3	3
25184	(1)	1	1	1	1
42586	(3)	3	3	3	3
48575	(4)	4	4	1	4
48431	(1)	1	1	0	1
48555	(1)	0	1	0	1
44208	(2)	2	2	2	2
12880	(27)	18	6	7	6
48944	(13)	12	0	0	0
57357	(1)	1	1	0	1
59442	(1)	1	1	1	1
48289	(1)	1	1	1	1
25124	(2)	1	1	1	1
43754	(2)	2	2	1	2
47796	(1)	1	1	1	1
41900	(1)	1	1	1	1
12660	(1)	1	0	0	0
44375	(1)	0	0	1	0
8571	(1)	1	0	0	0

تصویر 9: دسترسی به مقصد برای شبکه های در دسترس

Network	Addresses
ASK-AS Andishe Sabz Khazar Autonomous System (39308)	7
NGSAS Neda Gostar Saba Data Transfer Company Private Joint (39501)	4
TIC-AS Telecommunication Infrastructure Company (48159)	9
IR-PARSUN Parsun Network Solutions, IR (31732)	1
IR-AVABARID-AS Rasaneh Avabarid Private Joint Stock Company (51431)	1
AZADNET Azadnet Autonomous System (24631)	1
TEBYAN Tebyan-e-Noor Cultural-Artistic Institute (48434)	3
PAYAMAVARAN-KAVIR Shabakeh Gostar Payamavaran Kavir Company (Private Joint Stock) (57454)	1
PARSONLINE PARSONLINE Autonomous System (16322)	1
SINET-AS Soroush Rasanheh Company Ltd (21341)	6
FARAHOOSH Farahoosh Dena (44208)	1
DCI-AS Information Technology Company (ITC) (12880)	403
ASKHALIJFARSONLINE Khalij Ettela Resan Jonoub LTD (48944)	1
NEDA-AS neda rayaneh (30902)	1
IR-PISHGAMAN-ICP Pishgaman Kavir Yazd (34918)	2
HAMARA-AS Hamara System Tabriz Engineering Company (47262)	3
ASIATECH-AS AsiaTech Inc. (43754)	3
AFRANET AFRANET Co. Tehran, Iran (25184)	1
OFOGHNET-AS Mortabet Rayaneh Ofogh (29020)	1
FANAVA-AS Fanava Group (41881)	8

تصویر 10: شبکه های قابل شناسایی و سایت ها در فضای مسیریابی خصوصی



تصویر 11: شکست در انتشار سوابق DNS

تصویر 12: مسیر TraceRoute از میزبان 1

تصویر 13: مسیر TraceRoute از میزبان 2